3com

User Guide

Wireless LAN Access Points 8250/8500/8750

3CRWE825075A
3CRWE850075A
3CRWE875075A
(Models WL-450, WL-462, WL-463)

Version 2

http://www.3com.com/
http://www.3com.com/support/en_US/productreg/frontpg.html/

Published January, 2004
Version 2.3.12

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, and SuperStack are registered trademarks of 3Com Corporation.

Wi-Fi is a trademark of the Wireless Ethernet Compatibility Alliance.

All other company and product names may be trademarks of the respective companies with which they are associated.

EXPORT RESTRICTIONS: This product contains Encryption and may require US and/or Local Government authorization prior to export or import to another country.

Contents

2 System Configuration

INTRODUCTION

The 3Com® Wireless LAN Access Points 8250, 8500, and 8750 offer a dual-mode architecture that supports 802.11g, 802.11a and 802.11b wireless users on a single device. This means you can mix and match radio bands to meet different coverage and bandwidth needs within the same area. Different access point models give you the flexibility to choose to support both radio modes immediately or choose one radio mode now and upgrade to newer standards later as they become available with an easy-to-install optional Mini PCI upgrade kit.

With their flexibility and unfettered access, wireless LANs are changing the way people work. Now with 3Com's enterprise-class wireless access points, you can build a cost effective, reliable, secure wireless network that provides users with seamless connectivity to the Internet, company intranet, and the wired corporate network from anywhere they happen to be—conference room, cafeteria or office.

3Com's dual-mode design supports 802.11g, 802.11a and 802.11b wireless standards on a single access point. This capability increases configuration and coverage flexibility and protects your network investment for both existing and emerging wireless standards.

Industry-leading security features and comprehensive management and performance features combine to make these enterprise class wireless access points an ideal choice for organizations ready to serve their increasingly mobile workforce.

PRODUCT FEATURES

- **Access Point 8250**—Creates an enterprise-class wireless LAN supporting up to 250 simultaneous users. The single wireless interface 802.11g 2.4 GHz, 54-Mbps access point upgrades to 802.11g-802.11a dual mode with optional upgrade kit.
- **Access Point 8500—**Creates a high-performance enterprise-class wireless LAN supporting up to 250 simultaneous users. The single wireless interface 802.11a 5 GHz, 54-Mbps access point upgrades to 802.11b/g-802.11a dual mode with optional upgrade kit.

- **Access Point 8750**—Creates a high-performance enterprise-class dual-mode 802.11g and 802.11a wireless LAN supporting up to 250 simultaneous users up to 100 meters (328 feet).

SECURITY

3Com offers one of the most robust suite of standards-based security on the market today. To protect sensitive data broadcast over the wireless LAN, 3Com supports Wireless Equivalent Privacy (WEP) RC4 40/ 64-bit, 128-bit and 152-bit shared-key encryption. 3Com strengthens this basic security mechanism with additional security features, including MAC address access control lists, IEEE 802.1x per-port user authentication with RADIUS server authentication support, Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), Wireless Protected Access (WPA) and Extensible Authentication Protocol (EAP) support: EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP.

In addition to standards-based security, 3Com 128-bit Dynamic Security Link offers a high level of security, requiring a user name and password to access the wireless LAN.

PERFORMANCE AND RELIABILITY

3Com wireless access point performance features ensure reliable and seamless connections for users wherever they roam. Automatic channel selection automatically finds the least loaded channel for interference-free communication. Auto network connect and dynamic rate shifting keep users connected through a wide variety of conditions by changing to the optimum connection speed as they move through the network.

MANAGEABILITY

3Com offers a wide range of standards-based management support, from SNMP to 3Com Network Supervisor and HP OpenView for seamless integration with your wired network.

Wireless Infrastructure Device Manager and Wireless LAN Device Discovery tools let you configure parameters, run diagnostics, backup and restore configurations, and monitor performance from anywhere on the network using an embedded web server browser. You can also update wireless device software on multiple devices using 3Com Network Supervisor to simplify bulk updates.

With Power over Ethernet (PoE) support, the same Category 5 cable that connects your access point to the data network also provides its power. A single cable installation dramatically improves your choice of mounting configurations because you no longer

need to consider AC power outlet locations. PoE support makes it easier than ever to overcome installation problems with difficult-to-wire or hard-to-reach locations.

WIRELESS NETWORK STANDARDS

Understanding the characteristics of the 802.11g and 802.11a standards can help you make the best choice for your wireless implementation plans.

FAR-REACHING 802.11G

802.11g operates in the 2.4 GHz band at up to 54Mbps. Ratified in 2003, it supports the widest coverage—up to 100 meters (328 feet). However, is subject to a greater risk of radio interference because it operates in the more popular 2.4 GHz band.

Consider 802.11g when you need wider coverage and vendor compatibility and you are:

- Maintaining support for existing 802.11b users and the existing wireless investment while providing for expansion into 802.11g.
- Implementing a complete wireless LAN solution, including bridges, gateways, access points and clients; Wi-Fi certification guarantees compatibility among vendors
- Providing access to hot spots in public spaces such as coffee shops or university cafeterias

HIGH-PERFORMANCE 802.11A

Ratified in 2002, 802.11a is IEEE's more recent wireless standard. It operates at the 5 GHz band and supports data rates at up to 54 Mbps. For those organizations demanding even higher speeds, a "turbo mode" feature can boost throughput rates up to 108 Mbps. And because there are fewer devices in the 5 GHz band, there's less potential for RF interference. However, because it is at an entirely different radio spectrum, it is not compatible with 802.11g.

The higher spectrum provides about 50 meters (164 feet) of coverage—about half what 802.11g offers.

Consider 802.11a when you need high throughput in a confined space and you are:

- Running high-bandwidth applications like voice, video, or multimedia over a wireless network that can benefit from a fivefold increase in data throughput
- Transferring large files like computer aided design files, preprint publishing documents or graphics files, such as MRI scans for medical applications, that demand additional bandwidth

- Supporting a dense user base confined to a small coverage area. Because 802.11a has a greater number of non-overlapping channels, you can pack more access points in a tighter space.

NETWORK CONFIGURATION AND PLANNING

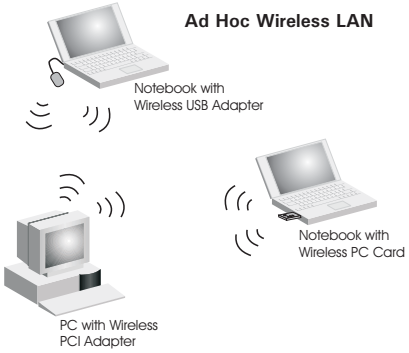
The wireless solution supports a stand-alone wireless network configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs.

The wireless network cards, adapters, and access point can be configured as:

- Ad hoc for departmental or SOHO LAN
- Infrastructure for wireless LAN
- Infrastructure wireless LAN for roaming wireless PCs

AD HOC WIRELESS LAN

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel. An ad hoc wireless LAN can be used for a branch office or SOHO operation.

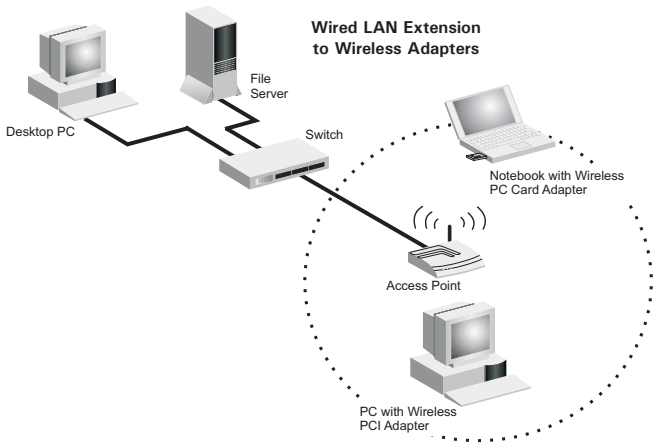


INFRASTRUCTURE WIRELESS LAN

The access point can also provide access to a wired LAN for wireless workstations. An integrated wired/wireless LAN is called an infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can talk to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via the access point.

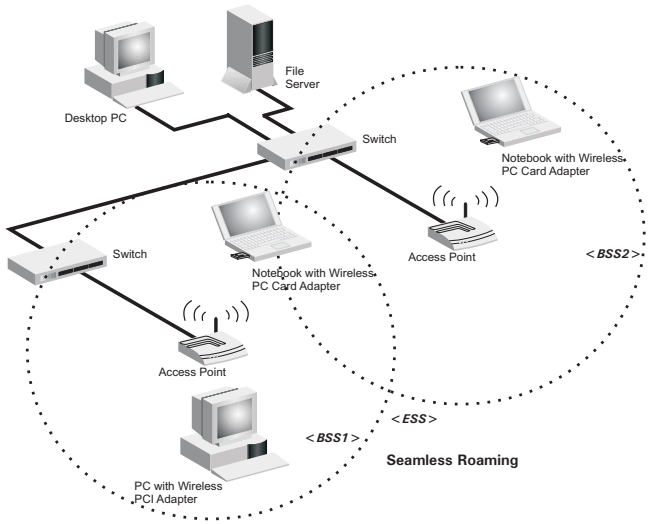
The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.



INFRASTRUCTURE WIRELESS LAN FOR ROAMING WIRELESS PCS

The Basic Service Set (BSS) is the communications domain for each access point. For wireless PCs that do not need to support roaming, set the domain identifier (SSID) for the wireless card to the SSID of the access point to which you want to connect. A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely.



TERMINOLOGY

Access Point—An internetworking device that seamlessly connects wired and wireless networks.

Ad Hoc—An ad hoc wireless LAN is a group of computers, each with LAN adapters, connected as an independent wireless LAN.

Backbone—The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Base Station—In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communications with the mobile radiotelephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station; each base station in turn is interconnected with other cells' bases.

BSS—Basic Service Set. It is an access point and all the LAN PCs that are associated with it.

CSMA/CA—Carrier Sense Multiple Access with Collision Avoidance.

EAP—Extensible Authentication Protocol, which provides a generalized framework for several different authentication methods.

ESS—Extended Service Set. More than one BSS is configured to become an ESS. LAN mobile users can roam between different BSSs in an ESS (ESS-ID, SSID).

Ethernet—A popular local area data communications network, which accepts transmission from computers and terminals.

Infrastructure—An integrated wireless and wired LAN is called an infrastructure configuration.

RADIUS—Remote Access Dial-In User Server is an authentication method used in conjunction with EAP for 802.1x authentication and session based keys.

Roaming—A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the infrastructure network.

RTS Threshold—Transmitters contending for the medium may not be aware of each other (they are "hidden nodes"). The RTS/CTS mechanism can solve this problem. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will not be enabled.

VLAN—Virtual Local Area Network. A LAN consisting of groups of hosts that are on physically different segments but that communicate as though they were on the same segment.

WEP—Wired Equivalent Privacy is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA—Wi-Fi Protected Access.

1 INSTALLING THE ACCESS POINT

This equipment must be installed in compliance with local and national building codes, regulatory restrictions, and FCC rules. For the safety of people and equipment, this product must be installed by a professional technician/installer.

***CAUTION**: Before installing, see the important warnings and cautions in "Safety Information" on page 14.*

INSTALLATION REQUIREMENTS

The following items are required for installation:

- Access Point 8250, 8500, or 8750
- Standard detachable antennas (Access Point 8250 and 8750)
- 3Com installation CD.
- Wall-mount installation hardware (supplied): mounting plate, mounting screws, and plastic anchors for drywall mounting.
- If you do not have IEEE 802.3af power-over-Ethernet LAN equipment, use the 3Com Integrated Power-over-Ethernet power supply that comes with the access point.

  If your LAN equipment complies with the IEEE 802.3af power-over-Ethernet standard, you can connect directly to the equipment, and the 3Com power supply is not needed.
- Standard category 5 straight (8-wire) Ethernet cable.

  The cable must be long enough to reach the power supply or the power-over-Ethernet LAN port.

  If you use the 3Com power supply, you need an additional Ethernet cable to connect the access point to the LAN.
- To access and use the Web configuration management system, you need a computer that is running Internet Explorer 5.0 or newer and one of the following operating systems: Windows 98, Windows ME, Windows NT 4.0 Service Pack 6, Windows 2000, or Windows XP. It is recommended that this computer become the dedicated

workstation for managing and configuring the access point and the wireless network.

POWER REQUIREMENTS

The access point complies with the IEEE 802.3af power-over-Ethernet standard. It receives power over standard category 5 straight (8-wire) Ethernet cable. Installation requires the use of either the 3Com power supply provided or IEEE 802.3af compliant power supply equipment (output power rated 48 V dc @ 350 mA maximum). Such equipment must be safety certified according to UL, CSA, IEC or other applicable national or international safety requirements for the country of use. All references to the power supply in this document refer to equipment that meets these requirements.

Because the power supply plug is the only means of disconnecting the access point from power, make sure the power outlet is accessible.

See "Using the Power Supply" on page 18 and "Using a Power-Over-Ethernet LAN Port" on page 19.

Note for use of the 3Com power supply (part number 61-0107-000) in Norway: This product is also designed for use on an IT power system with phase-to-phase voltage of 230 V.

SAFETY INFORMATION

This equipment must be installed in compliance with local and national building codes, regulatory restrictions, and FCC rules. For the safety of people and equipment, only professional network personnel should install the access point, cables, and antennas.

CAUTION: If you supply your own Ethernet cable for connecting power, be sure that it is category 5 straight-through (8-wire) cable that has not been altered in any way. Use of nonstandard cable could damage the access point.

CAUTION: To comply with FCC radio frequency (RF) exposure limits, a minimum body-to-antenna distance of 1 meter (3 feet) must be maintained when the access point is operational.

CAUTION: To avoid possible injury or damage to equipment, you must use either the provided power supply or IEEE 802.3af compliant power supply equipment that is safety certified according to UL, CSA, IEC, or other applicable national or international safety requirements for the country of use. All references to power supply in this document refer to equipment meeting these requirements.

CAUTION: The 3Com power supply (part number 61-0107-000) input relies on a 16A rated building fuse or circuit protector for short circuit protection of the line to neutral conductors.

CAUTION: It is the responsibility of the installer to ensure that the Power-over-Ethernet (POE) power supply is properly connected. Connection to any other device, such as a standard Ethernet card or another POE supply, may result in permanent damage to equipment, electric shock, or fire. Refer to the installation instructions for proper installation

DECIDING WHERE TO PLACE EQUIPMENT AND PERFORMING A SITE SURVEY

The access point is ideally designed for vertical installation on a wall surface, but can also be flat-surface mounted in an elevated location where it will not be disturbed. Ceiling installation is not recommended.

Whether you choose to mount the access point on a wall or place it on a flat surface, make sure to select a clean, dry location that is elevated enough to provide good reception and network coverage. Do not mount the access point on any type of metal surface. Do not install the access point in wet or dusty areas. The site should not be close to transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators or any other electrical equipment that can interfere with radio signals.

If you are connecting the access point to a wired network, the location must provide an Ethernet connection. You will need to run an Ethernet cable from the power supply to the access point.

An access point provides coverage at distances of up to 100 Meters (300 Feet). Signal loss can occur if metal, concrete, brick, walls, floors or other architectural barriers block transmission. If your location includes these kinds of obstructions, you may need to add additional access points to improve coverage

Configuring a wireless LAN can be as easy as placing a 3Com Wireless Access Point in a central area and making the necessary connections to the AP and the clients. However, installing multiple Access Points may require more planning. Using the 3Com Site Survey tool (located on the installation CD) can help you determine if your wireless LAN connectivity and throughput is adequate and all users are covered by an Access Point.

If you plan to use an optional antenna instead of the standard detachable antennas that are supplied, review “Selecting and Connecting a Different Antenna Model” on page 22 before selecting the final location and be sure to allow for routing the antenna cable as required.

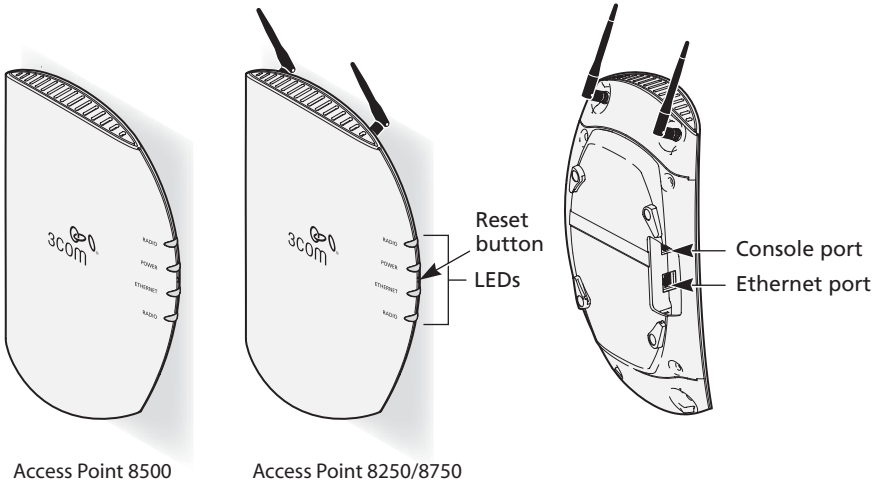
For optimal performance, ensure the access point operates in temperature ranges between –10° C to 40° C (14° F to 104° F). When used with external antennas, the access point operating temperature range must be 15° C to 40° C (59° F to 104° F).

Regulatory restrictions dictate that when this device is operational, the minimal body-to-antenna distance is 1 Meter (3 Feet).

BEFORE YOU BEGIN

Record the access point MAC address in a safe place before the access point is installed in a hard-to-reach location. The MAC address is printed on the back of the access point housing.

The following illustration shows the front and rear views of the access point, including the LEDs and connecting ports.



Caution: *Do not connect a telephone cable into the Console port; doing so can cause serious damage to the access point.*

CONNECTING THE STANDARD ANTENNAS

The Access Point 8250 and Access Point 8750 are supplied with standard detachable antennas. These should be attached before the access point is installed. If using an alternate antenna, see “Selecting and Connecting a Different Antenna Model” on page 22.

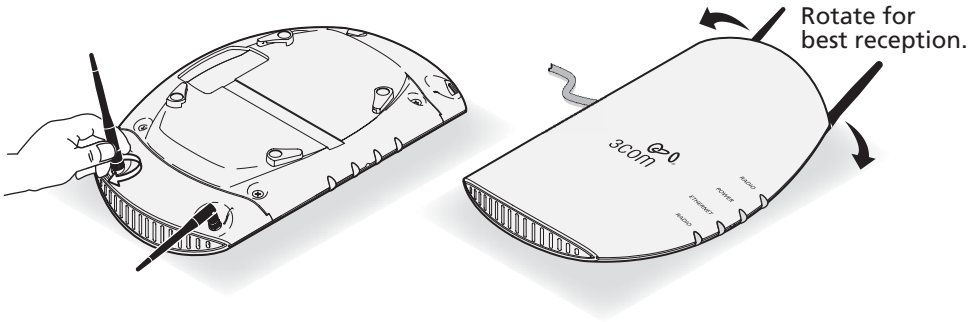
1 Carefully unpack the standard detachable antennas.

CAUTION: *Do not handle the antenna tips, especially after they are connected to the access point, as this could lead to electrostatic discharge (ESD), which could damage the equipment.*

2 Screw an antenna into each of the sockets in the access point housing.

3 Hand-tighten the antennas at the very base of the SMA connectors without handling the antenna tips.

4 Access Point 8250 and Access Point 8750: Position the antennas so they turn out and away from the access point at a 45-degree angle. After network startup, you may need to adjust the antennas to fine-tune coverage in your area.



Depending on the coverage required for your site, you may want to replace the standard detachable antennas with one of the external antennas available for use with the access point. See “Selecting and Connecting a Different Antenna Model” on page 22.

CONNECTING POWER

It is advisable to connect the power and check the Ethernet cables and LEDs before installing the unit in a hard-to-reach location.

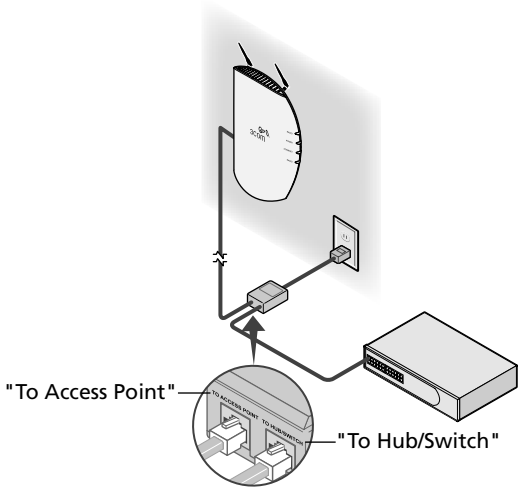
The access point complies with the IEEE 802.3af power-over-Ethernet standard. It receives power over a standard category 5 straight (8-wire) Ethernet cable.

There are two ways to supply power to the access point:

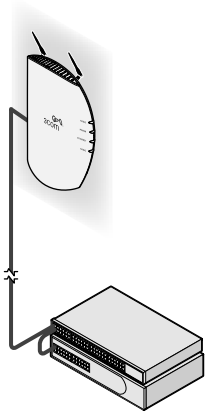
- Use the 3Com Integrated Power-over-Ethernet power supply. In this case, you need to supply a second Ethernet cable to connect to the wired LAN.

- Connect the access point directly to your own power-over-Ethernet hub or switch, which must also comply with the IEEE 802.3af standard.

  If you supply your own Ethernet cable for connecting power, be sure that it is standard category 5 straight-through (8-wire) cable that has not been altered in any way. Use of nonstandard cable could damage the access point.



Using the Power Supply



Using A Power-over-Ethernet LAN Port

USING THE POWER SUPPLY

CAUTION: *To avoid damaging network equipment, make sure that the cables are connected from access point to power supply to LAN as shown above and described below.*

The power supply can be located at any point between the access point and the LAN access port, wherever a convenient power outlet exists. If you supply your own Ethernet cable for connecting power, be sure that it is standard category 5 straight-through (8-wire) cable that has not been altered in any way. Use of nonstandard cable could damage the access point.

Refer to the illustration above, and follow these steps:

1 Connect one end of the Ethernet cable to the Ethernet port on the access point.

2 Connect the other end of the Ethernet cable to the port labeled *To Access Point* on the power supply.

3 Connect the power cord to the power supply and plug the cord into a power outlet.

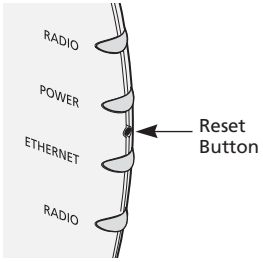
4 To link the access point to your Ethernet network, plug one end of another Ethernet cable into the port labeled To *Hub/Switch* on the power supply, and plug the other end into a LAN port (on a hub or in a wall).

USING A POWER-OVER-ETHERNET LAN PORT

If your LAN equipment complies with the IEEE 802.3af power-over-Ethernet standard, you can connect the access point directly to a LAN port. For example, the illustration above right shows a connection through a 3Com Ethernet Power Supply to a 3Com SuperStack® Switch.

CHECKING THE LEDS

When power is connected, the access point LEDs light. The illustration and the following table describe the LEDs and their functions.



Name	Description
Radio	LED blinks red to indicate radio activity. Faster blinking indicates more activity.
Power	LED lights green when operational code is running.
Reset Button	Press this button and hold for 15 seconds to restore the factory defaults.
Ethernet	LED lights yellow when Ethernet link is established. LED blinks to indicate activity on the Ethernet. Faster blinking indicates more activity.
Radio	LED blinks red to indicate radio activity. Faster blinking indicates more activity. (This LED is only active when a second radio is installed.)

MOUNTING ON A WALL

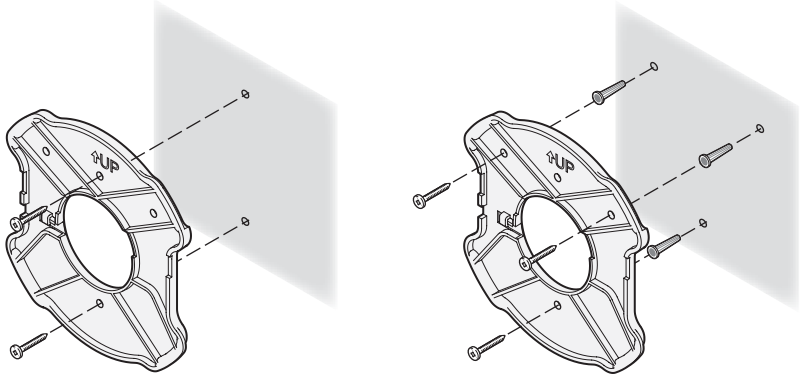
CAUTION: *The mounting plate is designed for wall mount installation only. To avoid equipment damage and possible injury, do not use the mounting plate for a ceiling installation.*

The access point comes equipped with all the necessary hardware for mounting on a wall, including a mounting plate. For a secure installation, the mounting plate should be placed perpendicular to the floor, with the arrow pointed up, as indicated on the mounting plate, with the smooth side against the wall.

1 Install the mounting plate as shown in the following illustration, on either a stud (or other hard wall surface), or onto drywall.

If installing into a stud or other secure vertical surface, use 2 screws.

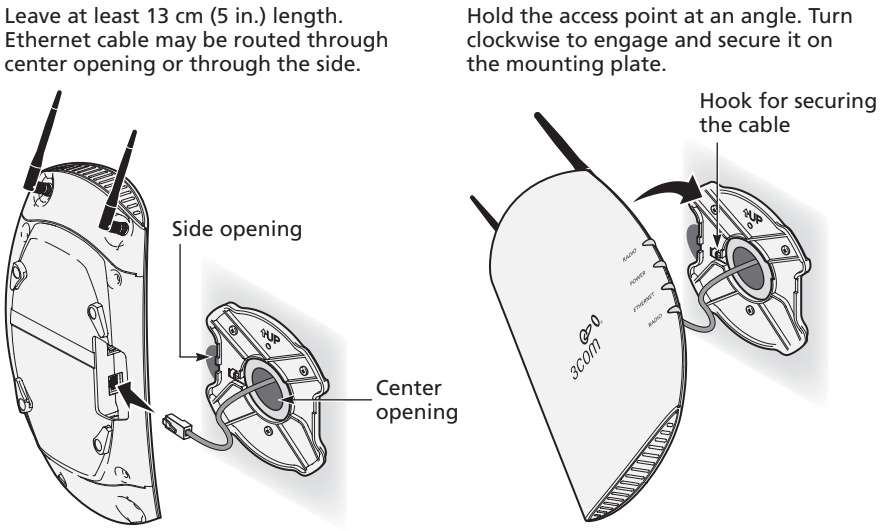
If installing into drywall, use 3 plastic anchors and 3 screws.



- Allow for a clearance of at least 25 cm (10 Inches) between the ceiling and the top of the mounting plate.
- Make sure that “UP” or “A” is oriented toward the top of the bracket, and align the mounting plate screw holes vertically.
- For installation on a wall stud, install the top screw into the stud, as shown at left in the illustration, and then vertically align the mounting plate before installing the bottom screw.
- For installation on to drywall, mark three screw holes using the mounting plate as a template for vertical alignment, as shown at right in the illustration above.
- Use a 5-mm (3/16-in.) drill bit if using the plastic anchors provided.
- For drywall mounts, you can route the cable through either a side or center opening for a seamless appearance using one of the methods illustrated below. Alternatively, you can simply attach the Ethernet cable to the side of the unit, allowing it to trail along the wall.
- If you have routed the Ethernet cable through the center opening, secure the cable on the hook located on the mounting plate as shown in the illustration below.

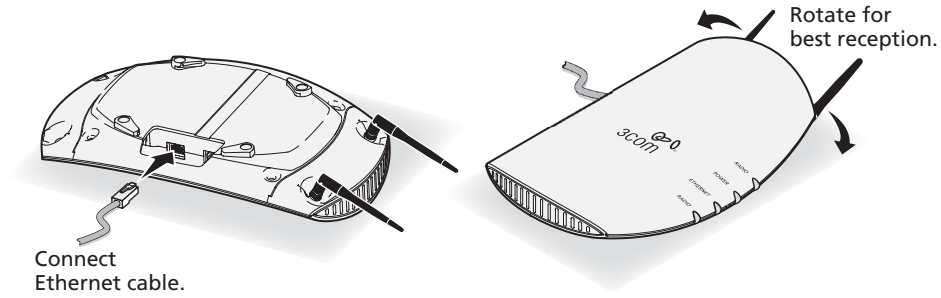
2 Connect the Ethernet cable to the Ethernet port on the access point.

3 Position the access point at an angle to the mounting plate bayonet connection and turn the unit clockwise until it snaps into place, as shown below.



FLAT SURFACE INSTALLATION

The access point can also be placed on a flat surface such as a table, desktop or filing cabinet. Do not install the access point on any type of metal surface. If you choose a flat surface mount, select a location that is clear of obstructions and provides good reception.



***Note**: Regulatory restrictions dictate that when this device is operational, the minimal body-to-antenna distance is 1 Meter (3 Feet).*

SELECTING AND CONNECTING A DIFFERENT ANTENNA MODEL

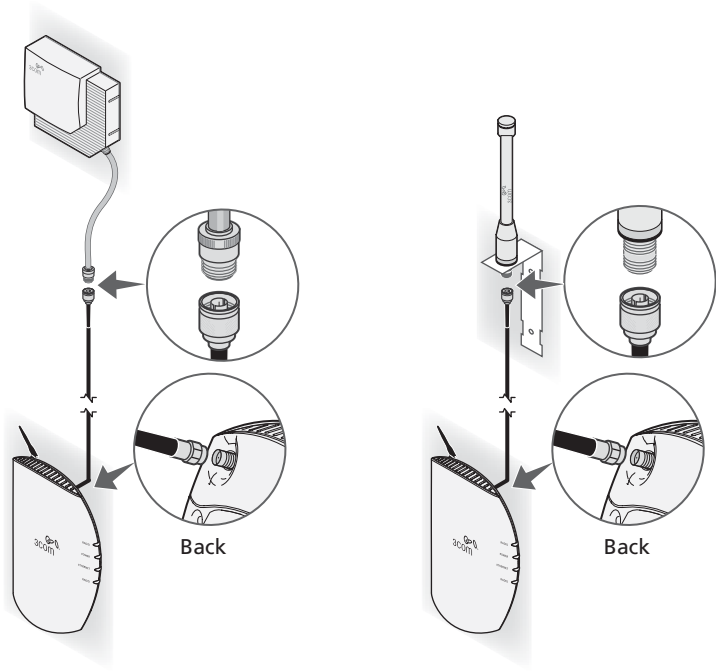
***Note**: For FCC regulatory compliance reasons, in the United States, Canada, and other countries governed by FCC guidelines, external antennas can only be used in an access point operating temperature range of 15° C - 40° C (59° F - 104° F).*

***Note**: If the access point is used with an external antenna you must also purchase an antenna cable. For maximum efficiency, use the shortest antenna cable possible. Antenna cables induce signal loss, which will limit the radiated power output and range of the access point. Of the options available, we recommend the 3Com 6-foot Antenna Cable (3CWE480).*

The standard detachable antennas supplied with the Access Point 8250 and Access Point 8750 are suitable for a broad variety of environments. If you require a different type of antenna for the Access Point 8250 or Access Point 8750, several options are available by model number from the 3Com Web site (www.3Com.com). (Access Point 8500 does not support interchangeable antennas.)

For each of the antenna models, you will need either a 6-foot accessory cable (model 3CWE480) or a 20-foot accessory cable (model 3CWE481) to provide the transition from the SMA connector on the access point to the N-type connector on the antenna.

To ensure the physical safety of anyone near the antenna and to prevent damage to the access point, follow the building codes for antenna installations in your area. Also, when connecting the optional antenna to the access point, remember to use only the A-side connector on the access point, on the right when properly installed.



1 Position the antenna so that there are minimal obstacles between it and any client with which it will communicate. While maintaining a direct line of sight between the antenna and a client is not strictly necessary, such an arrangement helps to ensure a strong signal. Ensure that access is available for routing the antenna cable from the antenna to the access point.

2 If they are installed, remove both arms of the standard detachable antenna, making sure not to handle the tips of the antenna.

3 Connect one end of the optional antenna cable to the antenna and secure the antenna in place.

4 Connect the free end of the antenna cable to the right-hand side connection on the access point, as shown in the illustration above.

5 Make certain that the antennas and antenna masts are appropriately grounded to prevent injury or damage from lightning strikes.

POWER SETTINGS ON THE ACCESS POINT FOR EXTERNAL ANTENNAS

USA

	2.5dBi (3CWE492)	4dBi (3CWE490, 3CWE497)	8dBi (3CWE491, 3CWE498)
6 ft (3CWE480)	100%	100%	100%
20ft (3CWE481)	100%	100%	100%
50 ft (3CWE482)	100%	100%	100%

European Community

	2.5dBi (3CWE492)	4dBi (3CWE490, 3CWE497)	8dBi (3CWE491, 3CWE498)	13dBi (3CWE495)
6 ft (3CWE480)	100%	100%	25%	12.5%
20ft (3CWE481)	100%	100%	100%	25%
50 ft (3CWE482)	100%	100%	100%	100%

INSTALLING SOFTWARE UTILITIES

The installation CD includes documentation and software utilities to help you set up and administer the wireless components of your network.

To view product documentation, select *View the Documentation* from the CD Startup Menu and then select the item you wish to view.

The software Tools and Utilities include:

- **3Com Wireless Infrastructure Device Manager.** Use this tool to discover access points and select devices for administrative changes.
- **3Com 3CDaemon Server Tool.** This tool can act in four different capacities:
  - As a TFTP Server, necessary for firmware upgrades, and backup and restore functions. Use this option if you do not have a TFTP server set up.
  - As a SysLog Server, which is necessary to view SysLog messages.
  - As an optional TFTP Client.
  - As an optional FTP Server.
- **3Com Network Supervisor.** The 3Com Network Supervisor (3NS) graphically discovers, maps, and displays network links and IP devices, including 3Com wireless access points. It is not required for access point management.
- **3Com Site Survey Tool**. This utility assists in selecting the best location for your access point before installing the device permanently. Use the Site Survey Tool to determine if the intended mounting locations will provide adequate coverage with good signal strength and quality.
- **Internet Explorer 5.5.** This browser is included for those who do not have a suitable browser.

To install a tool from the CD:

1. Power up the computer and put the 3Com CD in the CD-ROM drive.
2. The setup menu should appear when the CD autostarts. If no menu appears, you can run the setup.exe startup program from the Windows Start menu. For example, if your CD drive is the D drive: Start / Run / d:setup.exe.
3. From the CD startup menu, select *Tools and Utilities*.
4. Select the item you want to install and follow the instructions on the screen.

2 SYSTEM CONFIGURATION

The access point can be configured using a Web browser that has Java support (Internet Explorer 5.0 or newer). Using the Web management interface, you can configure the access point and view statistics to monitor network activity.

The 3Com Wireless Infrastructure Device Manager helps you locate 3Com wireless LAN devices on the network, select a device and view its properties, and launch the device's configuration in your Web browser. To configure a device, the device manager must be installed on a computer that has an Ethernet adapter and is running a supported Windows operating system and Web browser.

USING THE 3COM WIRELESS DEVICE MANAGER

After the 3Com Wireless Device Manager is installed, ensure that the device to be configured is either wired to the network, associating with the wireless network, or connected directly to the computer, and connected to power. If more than one device using the factory default name is connected, make a note of the MAC address of the device you want to select so that you can identify it in the device manager.

LAUNCHING A WIRELESS DEVICE CONFIGURATION

If you do not have a DHCP server on your network, it can take up to one minute for a device to become discoverable after it has been powered up.

1 To launch the 3Com Device Manager, select *Start /Programs /3Com Wireless/Wireless Infrastructure Device Manager*.

If you have more than one network adapter installed on your computer, you may be prompted to choose a network adapter. Choose the appropriate adapter and click *OK*.

The Wireless Network Tree appears in the 3Com Wireless Infrastructure Device Manager window. The tree lists all WLAN service areas on the network and expands to show the 3Com wireless LAN devices that are associated to each service area. Devices in a different subnet than your computer are identified with

exclamation points (!). You can refresh this display by clicking *Refresh*. You should refresh the display, for example, after you change a device IP address.

2 In the Wireless Network Tree, select the device you want to configure.

If more than one wireless LAN device appears in the tree and you are not sure that you have selected the right one, click *Properties* and check the MAC address to verify that it is the one you want.

3 Click *Configure*.

- If the selected device is on the same subnet as your computer, the configuration management system main page appears in your Web browser. (If a password is set on the device, enter it when prompted.)
- If the selected device is on a different subnet, the Pre-IP Configuration Wizard is activated automatically. This wizard lets you configure the IP settings for the selected wireless device. It proposes IP address and subnet mask settings derived from your computer's settings, so the selected device will then reside on the same subnet as your computer. You can accept the suggested settings or change them as required. For more information, see "Using the Pre-IP Configuration Wizard" on page 28.

The next window prompts for an administrative password to allow the new IP address to be set. When the units are shipped from the factory, there is no administration password and you should leave the password field blank. If an administration password has been set for the device, enter the password and click *Next*. The 3Com Web Configuration Management System main screen appears in your Web browser.

The following table describes the functions of the buttons in the 3Com Wireless Infrastructure Device Manager window.

Button	Description
Properties	Displays the following properties of the selected device: Device Name, Device Type, Wireless LAN Service Area (ESSID), IP Address, Subnet Mask, and MAC Address.
Configure	Launches the Configuration Management System for the selected device. If the selected device is on a different subnet, you are prompted to assign an address on the same subnet as your computer.
Refresh	Scans the network and displays the connected 3Com 11 Mbps Wireless LAN devices.
Choose NIC	If your computer has more than one network interface card installed, allows you to choose which card you want to use.
Close	Closes the device manager window and ends the session.
Help	Launches the device manager help page in your browser.

USING THE PRE-IP CONFIGURATION WIZARD

You can only configure devices that are on the same subnet as your computer. To configure a device on a different subnet, you must first assign it an IP address on the same subnet as your computer. After you launch the configuration, you can change settings as usual. Just before you finish, you must change the device IP address back to its original setting. Follow this procedure:

1 In the Wireless Infrastructure Device Pre-IP Configuration window, accept the suggested settings or change them as required. You can assign a static IP address or specify that the device obtain its IP address from a DHCP server.

2 The next window prompts for an administrative password. When the units are shipped from the factory, there is no administration password and you should leave the password field blank. If an administration password has been set for the device, enter the password and click *Next*. The Configuration Management System main page appears in the Web browser.

CONFIGURATION LOGIN

After you launch the configuration from the device manager, the login page appears in your browser. The default Username is admin and the default password is no password. For an initial configuration, enter the default Username and click *LOGIN*. Then set the Country Code as described below.

SETTING THE COUNTRY CODE

The Country Code determines the available channels and transmission power level based on regulatory restrictions in the country where the access point is installed. The first time you log in, you must set the Country Code.

To ensure compliance with local regulations, be sure to select the country in which the access point is installed.

In the Country Code page, select the country from the pull-down list and click *Apply*. The Home page appears.

BASIC SETUP

For a basic configuration, use the Setup Wizard as described below.

At any time, you can click Home to return to the Home page of the configuration interface. If you want to configure more advanced features, click Advanced Setup in the Home page.

1. In the Home page, click *Setup Wizard.*
2. In the "1-2-3" Setup Wizard page, click *Next* to start basic configuration.
3. In the SSID page, enter the same Service Set ID as the other wireless devices in your network and click *Next.* (The SSID may be up to 32 alphanumeric characters and is case sensitive.)
4. In the Channel page, select the channel options for the access point radios and click *Next.* The channel options are:

   802.11g—You can select from these options:

   - 802.11g Radio Channel—Set the operating radio channel number.
   - Auto Channel Select—When this mode is enabled, the access point selects a radio channel automatically.

   802.11a—You can select from these options:

   - Turbo Mode—In some countries you can use Turbo Mode, allowing the access point to operate with a data rate of up to 108 Mbps. If Turbo Mode is not allowed in your country, this option is not available.
   - 802.11a Radio Channel—Set the operating radio channel number.
   - Auto Channel Select—When this mode is enabled, the access point selects a radio channel automatically.

   802.11b—Set the operating radio channel number.
5. In the TCP/IP Settings page, you can choose whether the access point obtains its IP address from a DHCP server or uses a static IP address. Configure the DHCP Client settings and click *Next.*
6. In the Security page, make selections and click *Next.*

   For details on security settings, see "Security" on page 42.
7. Click *Finish.*
8. Click *OK* to restart the access point.

ADVANCED SETUP

The Advanced Setup pages allow you to configure features that are not available in the basic setup. On the Home page, click *Advanced Setup* to open the Advanced Setup menu.

After making selections and entering data on each page, click *Apply* to save the changes.

The following sections describe the Advanced Setup pages.

IDENTIFICATION

On the Identification page, you can identify the access point by providing a descriptive name. This name then appears in the device manager window. Enter a maximum of 32 alphanumeric characters in the System Name field and click *Apply.*

TCP/IP SETTINGS

On the TCP/IP Settings page, you can configure TCP/IP (Transmission Control Protocol/Internet Protocol) settings as described below. When you are finished configuring items on this page, click *Apply.*

DHCP CLIENT

When DHCP (Dynamic Host Configuration Protocol) Client is enabled, and a DHCP server is located on the network, the network DHCP server assigns the IP address, subnet mask and default gateway to the access point.

If there is no DHCP server on the network, the access point automatically uses its default IP address, 169.254.*2.1*.

When DHCP Client is disabled, you can specify the IP setup as follows:

- **IP Address** and **Subnet Mask**—If you configure an IP address and subnet mask, you must configure the network settings of the computers on your wireless LAN to use the same subnet mask. The IP addresses specified must be valid on the same subnet.
- **Default Gateway**—The default gateway address is optional, but may be required by your Internet Service Provider.
- **Primary DNS Address** and **Secondary DNS Address**—The Domain Name Servers (DNS) map numerical IP addresses to the equivalent domain name (for example, www.3Com.com). Your internet service provider should provide the IP

address of one or more domain name servers. Enter those addresses in Primary DNS Address and Secondary DNS Address fields.

SECURE WEB SERVER CONNECTION

This option controls whether Secure Socket Layer (SSL) technology is used to encrypt information between the computer and the device during a configuration session. By default this option is Off. When this option is turned on, the HTTPS protocol is used, and data is protected during the configuration session. When it is turned off, the HTTP protocol is used, and data could be intercepted during the configuration session.

Changing this option causes the device to reset, which disrupts the network association temporarily, but does not affect device configuration settings that have already been saved.

RADIUS

The RADIUS page lets you define servers to be used for authentication and accounting. RADIUS (Remote Access Dial-In User Service) is a login authentication protocol that uses software running on a central AAA (Access, Authentication, and Accounting) server to control access to RADIUS compliant devices on the network. There are no special settings on the access point to distinguish between the various RADIUS policies or authentication types (for example EAP-MD5, EAP-TLS, EAP-TTLS). These policies are setup and controlled on the AAA server. Note that for most RADIUS software packages, the access point is actually called the "RADIUS client" and has a shared secret or secret key corresponding to the RADIUS setup page (see *KEY* parameter below).

The access point can send connection parameters to a RADIUS server, as well as statistics for accounting purposes. The access point is compatible with RFC2866 (the RADIUS Accounting specification).

Configuring a secondary RADIUS server provides a backup in case the primary server fails. The access point will use the secondary server if a failure is detected in the primary server. Once the access point switches over to the secondary authentication server, it periodically attempts to establish communication again with primary authentication server. Once communication is established, the secondary authentication server reverts back to a backup server. The access point will use the secondary accounting server if a failure is detected in the primary accounting server. It will continue to use the secondary accounting server until it fails, in which case it returns to sending data to the primary accounting server.

See here for recommended steps in configuring RADIUS Authentication.

In the RADIUS Authentication section, enter the required parameters for a primary and secondary RADIUS authentication server.

In the RADIUS Accounting section, click the *Enable* radio button, then enter required parameters for a primary and secondary RADIUS accounting server.

When you are finished configuring items on this page, click *Apply.*

The parameters are described below.

- **IP Address**—The address of the server.
- **Port**—The network (UDP) port of the server used for messages. The port defaults to 1812 (1813 for RADIUS Accounting) and must match the port configured on the RADIUS server.
- **Key**—The encryption key is a shared ASCII string that is used to authenticate logon access for the client. The maximum length is 255 characters. Do not use blank spaces in the string. The key must be configured the same on both the access point and the RADIUS server. The Authentication and Accounting RADIUS servers can have different secret keys.
- **Timeout**—The number of seconds the access point waits for a reply from the RADIUS server before it resends the request.
- **Retransmit attempts**—The number of times the access point will try to authenticate logon access.
- **Update Interval**— (RADIUS Accounting Only) This is the interval in seconds between accounting updates sent to the RADIUS accounting server.
- **Accounting Log Options**— (RADIUS Accounting Only) This option controls which clients will generate accounting logs. If set to RADIUS Authenticated Clients Only, only those clients which successfully complete 802.1x Authentication will generate accounting logs. The default is for all authenticated clients to generate accounting logs.

AUTHENTICATION

The Authentication page allows you to configure the type of upper-layer authentication the access point uses for wireless clients. This authentication setup is applicable for **both** radio interfaces. Access is checked against the MAC Address authentication database stored on the access point.

NOTE: This level of authentication occurs **BEFORE** any 802.1x authentication configured on the Security page. When using Local and RADIUS MAC Authentication, clients attempting to authenticate to the access point **MUST** pass these settings before any subsequent 802.1x authentication is attempted and verified. If no MAC address filtering is desired, leave this set to the default setting of Disable.

Configure the options as described below. When you are finished, click *Apply*.

- **MAC Authentication**— Selecting MAC authentication allows you to define access permission and precedence. Options are:

  Local MAC— With this option, the MAC address of the associating station is compared against the local access control list. You must build this list (called the MAC Authentication Table) as described in Local MAC Authentication below. Use this option if you want to restrict wireless clients authentication to the access point based off their MAC address.

  RADIUS MAC— With this option, the MAC address of the associating station is sent to the configured RADIUS server for validation. You must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. See “RADIUS” on page 31 and “802.1x Wireless Setup” below.

  Disable— No MAC address related checks are performed on a client requesting authentication to the access point.

- **802.1x Wireless Setup**—802.1x is designed to enhance the security management of the wireless network. Select one of the following options:

  Disable— The access point will neither initiate nor respond to any 802.1x authentication requests to or from wireless clients.

  Supported — Legacy clients (non 802.1x) and 802.1x clients are both supported. This is provided for ease of migration. This option works with WPA key management set to either “WPA authentication over 802.1x” or “WPA pre-shared key (PSK)” on the radio security page.

  Required — Clients authenticate to a RADIUS server via the access point. Clients are not allowed onto the wired LAN until authentication is successful. If two Radios are installed and WPA is being used, both radios’ security must be set to “WPA authentication over 802.1x” for the WPA key management when 802.1x is Required. If one radio’s security is set to “WPA pre-shared key (PSK)” for WPA key management and the other is “WPA authentication over 802.1x”, then the 802.1x Wireless Setup must be set to “Supported” instead.

  When 802.1x is enabled, the broadcast and session key rotation intervals can also be configured. Set these values to force the periodic refresh of broadcast or session keys for each 802.1x client.

  First set up the RADIUS authentication for the client on the RADIUS authentication server. (See “RADIUS” on page 31.) Select Supported or Required on the 802.1x Wireless Setup field above. Enter data as described in the following table.

Field	Default	Description
Broadcast Key Refresh Rate	0 (minutes)	Defines how long the RADIUS server will refresh the primary broadcast key.
Session Key Refresh Rate	0 (minutes)	Defines how long the RADIUS server will dynamically re-assign a session key to a connected client station.
802.1x Reauthentication Refresh Rate	0 (seconds)	Defines the time interval in which the Access Point forces a Reauthentication and subsequently re-issues a new session key.

- **Access Point 802.1x Authentication to Network**—802.1x can also be enabled on the ethernet port of the switch that the access point's ethernet cable is plugged into. Having 802.1x enabled on the switch prevents any device that is not able to successfully authenticate from being able to use the ethernet port. This option is useful if your access point is located in an insecure location, and you want to prevent someone who plugs a computer or another access point into the network connection being used by your access point from being able to access the network. This feature defaults to being disabled.

  If "MD5 Authentication to Network with MAC Address" is selected, the access point's MAC address will be used for both the username and password. For example, an access point with the MAC Address 12-34-56-78-9A-BC would use a username and password of "123456789abc".

  If "MD5 Authentication to Network with Supplied Username and Password" is selected, the access point with authenticate using the username and password supplied. If you press the "Apply" button when no password is specified, the previous password will continue to be the one used. You must enter the same password twice to successfully change the password.
- **Local MAC Authentication**—Client computers can be filtered using the unique MAC addresses of their network cards. To build the MAC Authentication Table, enter a MAC address in the space provided, choose the permission, and click *Update.* MAC addresses are listed in the MAC Authentication Table in the order that they were entered. The Local MAC Authentication parameters are described in the following table:

Parameter	Description
System Default	Define the default filtering setting as Deny or Allow.

Parameter	Description
MAC Address	Enter the MAC address of a client for the access control. You can find the MAC address of a network card as follows: **Windows 95/98/ME**—Click *Start/Run.* Type winipcfg and press *Enter.* The MAC address is in the Adapter Address section. **Windows NT4/2000/XP**—At the command prompt, type ipconfig /all and press *Enter.* The MAC address is listed as the Physical Address. **Linux**—Run the command "/sbin/ipconfig." The card's MAC address is the value after the word "HWaddr."
Permission	Allows or denies access to the access point of devices matching the specified MAC address.
Update button	Click *Update* to refresh the MAC Authentication Table. To avoid the possibility of entering an invalid MAC address on the Authentication page, always click *Update* after typing the address. If you press *Enter,* address error checking does not occur.

FILTER CONTROL

The Filter Control page allows you to control client communication within the wireless network. You may enable one or more types of supported filtering; however, some filter choices may supersede others. Configure the options as described below. When you are finished, click *Apply.*

FILTERING BY VLAN

The access point supports filtering of up to 64 VLANs (virtual local area networks). VLAN IDs must be configured for each client on one of the RADIUS authentication servers specified on the RADIUS configuration page. If a RADIUS server is not being used or not setup to update the VLAN ID, then the access point will tag all ethernet packets with the Native VLAN ID (defaulted to 1).

If a RADIUS authentication server will be used to create/modify the VLAN ID, the following attributes must be provisioned on the RADIUS Server to be passed back to the authenticating client:

The AP's IP address is the RADIUS Client/Radius User

Tunnel_type (64) = VLAN (13)

Tunnel_Medium_type (65) = 802

Tunnel_Private_group_ID (81) = VLAN ID specified in Hexadecimal format.

VLAN Switch ports must be tagged ports that match the VLAN ID on the Access Point. Associated client VLAN IDs will appear in the Syslog file in ASCII Decimal format.

When VLAN filtering is enabled, the access point queries the server for the VLAN IDs of associating clients and saves the VLAN IDs. If a client does not have a VLAN ID, the access point assigns its own native VLAN ID to that client.

To enable VLAN filtering, enter a VLAN ID (a number between 1 and 4095) in the *Native VLAN ID* field and select *VLAN Enable.*

When VLAN filtering is disabled, the access point ignores VLAN-tagged frames.

SECURITY FILTERS

These options allow you to block communication among wireless clients (client-to-client blocking) and prevent wireless clients from performing access point administration.

- **Local Bridge Filter**—Enable this filter to prevent direct communication between wireless clients, creating a more secure wireless network.
- **AP Management Filter**—Enable this filter to prevent wireless clients from accessing the access point for management; for example through TELNET or SNMP.

CLIENT LIST TIMEOUT

This option sets the timeout for inactive clients to be disassociated and removed from the associated client list. The interval can be set to 1, 5, 10, 30 or 60 minutes (default is 30 minutes).

UPLINK PORT MAC ADDRESS FILTERING

This feature allows associated wireless clients to communicate only with specific selected MAC addresses on a sub net. By only allowing clients to communicate with a few specific servers such as DHCP server, a Gateway, or a local web server, clients are blocked from communicating with other clients on the local sub net, but are still allowed (via the gateway) to communicate with severs on the Internet. **Note:** In most cases client to client blocking should also be enabled as the *Uplink Filter* only works on packets coming into the AP from its Ethernet (uplink) port.

For security reasons it is desirable to block client to client communications for wireless clients associated with an Access Point (AP). It is also desirable to block client to client communications between clients associated with different AP's on the local sub net. For instance an airport may have several AP's to service several "hot spots" within

the airport. However the client to client blocking feature of the AP will only block communications to other clients associated with the same AP. And will not block client to client of another AP communications. By using the *Uplink Filtering* function of the AP communications to all other clients of all other AP's on the same sub net can be blocked.

It is important to note that this feature only works if all the AP's are on the same sub net. If an AP is located on the far side of the gateway (i.e. on a different sub net) its clients will NOT be blocked from communicating with clients on the local sub net of interest.

This feature is accessed on the Filter Page of the user interface. Click on the Uplink Filter List link and add up to eight MAC addresses that WILL be allowed to communicate with clients of the AP. Make sure to include the MAC of the local DHCP server, if it not the same as the gateway as well as and redirect gateways and other servers that should be allowed to communicate with the AP's wireless clients. Make sure to click on the save button on both the Uplink Filter List page as well as the Filter page to activate the function.

FILTERING BY ETHERNET PROTOCOL TYPE

Use the Ethernet Type Filter table to filter out Ethernet packet frames that match the Ethernet protocol type. Select *Ethernet Type Filter Enable,* then set the status of each Ethernet frame type in the list.

Although there are five types of IPX packets, the Filter Control page shows only two options for IPX filtering. The following table shows how to filter each IPX packet type:

ISO Designator	Filter
8138	Enable 8138
8137	Enable 8137
802.3(Raw)	Enable 8138
802.2	Enable 8138
SNAP	Enable 8137

SNMP

Use the SNMP page to display and enter a community string for the Simple Network Management Protocol. To communicate with the access point, the SNMP agent must first be enabled and the Network Management Station must submit a valid community

string for authentication. Select SNMP Enable and enter data into the fields as described below. When you are finished, click *Apply.*

- **Location**—Specifies the access point location.
- **Contact**—Sets the system location string that describes the system location. (Maximum length: 255 characters)
- **Community Name (Read Only)**—Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. (Maximum length: 23 characters)
- **Community Name (Read/Write)**—Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. (Maximum length: 23 characters)
- **Trap Destination IP Address**—Fill in the IP address box for a trap manager that will receive these messages.
- **Trap Destination Community Name**—Fill in the community string box for a trap manager that will receive these messages. (Maximum length: 23 characters)

ADMINISTRATION

The Administration page allows you to perform access point management tasks as described below.

- **Change Password**—A password is required to configure the access point. Enter the user name and new password in the spaces provided and click *Apply.* It is recommended that you change the password from the default value (no password) to ensure network security.
- **Firmware Upgrade**—You can upgrade firmware from a downloaded file that you have placed on the local computer, or from a remote FTP or TFTP server.
  - **Local**—Click *Browse* to locate the downloaded firmware file. Click *Start Upgrade* to start the upgrade process. The upgrade takes place through the HTTP protocol from the local machine.
  - **Remote**—Select FTP or TFTP. Enter the firmware file name, the host IP address where the file is stored, the user name, and the password. Click *Start Upgrade* to start the upgrade process.
- **Backup and Restore Configurations**—Access point configurations can be saved as data files and later used to restore the access point configuration. This option lets you save access point settings in an external file or copy them from an external file to the access point. You can save an entire configuration for use as a backup to a single access point, or you can save a basic configuration, which can then be used in common by several access points in a network, providing an easy way to reconfigure all access points in a network.

  You must have a TFTP server set up on which to store the backup files.

To back up a configuration — Type the IP address of the TFTP server and a name for the backup file in the spaces provided. Click *Basic* (to save a partial configuration) or *Complete* (to save an entire configuration) and click *Backup Configuration*.

To restore a configuration — Type the IP address of the TFTP server and the name of the backup file in the spaces provided and click *Restore Configuration.* Restoring a configuration causes the access point to reset. If the file being restored was saved as a Basic configuration, only general configuration parameters such as SSID, country code, radio settings, security settings, RADIUS server settings, and management setup information are restored. Parameters that are unique to individual access points, such as device names, IP addresses, and administration passwords, are neither affected nor overwritten.

Before restoring a configuration you can view a description of the restoration point by clicking the *Restore User Comment* button. Comments made at the point the backup was created will appear in the "User Comments" field. This feature allows the user to select the correct restoration point.

To restore comments — Click the Restore Comments button to view comments saved on previous backups.

- **Factory Settings**—Click *Restore* to load the factory default configuration and reboot the access point. All user-configured information is lost. You must reenter the default user name (admin) to regain management access to this device.
- **Reset Access Point**—Click *Reset* to perform a hardware reset of the access point. Current configuration settings are not changed.

SYSTEM LOG

The System Log page allows you to set up a server to store event logs and to specify how the access point obtains the date and time. When you are finished configuring items on this page, click *Apply.*

Each logging message is tagged with a severity level, as defined in RFC3164. The severity levels are:

- Emergency: system is unusable
- Alert: action must be taken immediately
- Critical: critical conditions
- Error: error conditions
- Warning: warning conditions
- Notice: normal but significant condition
- Informational: informational messages
- Debug: debug-level messages

To set up a server for event logs: Select *System Log Setup Enable,* select a logging severity level from the pulldown list, enable the Logging Host and Logging Console, and enter the IP address of the server in the space provided.

To designate an SNTP server for obtaining the date and time: Select *SNTP Server Enable* and enter the IP addresses for primary and secondary SNTP servers in the spaces provided.

To use the access point as an SNTP server: Select *SNTP Server Disable,* specify time values in the spaces provided, select the time zone from the pull-down list. If you check the *Enable Daylight Saving* check box, the time will adjust automatically for standard and daylight saving time. When the SNTP Server setting is disabled, date and time settings revert to the defaults after an access point is reset, affecting the accuracy of log reports. To avoid this situation, enable the SNTP server setting and allow the access point to obtain the date and time from an SNTP server. (The event log page will display the default time after a reset until the access point receives the correct information from the SNTP server.)

STATUS

The Status pages display additional information about the access point status and station status.

- **AP Status**—Click *AP Status* to view the access point system configuration and access point wireless configuration.
- **Stations Status**—Click *Stations Status* to view the configurations of connected stations. The Station Status page displays basic connection information for all associated stations. Select “refresh” on you browser to see update station status.
- **Event Logs**—Click *Event Logs* to display the activity log of the access point. The event log resets to zero if the access point is reset or the *Clear Event Logs* button is pressed. The log saves 128 events, then overwrites the first event and continues.

RADIO INTERFACE

The access point radio interface detects the number of radios installed and their type (802.11g Radio, 802.11a Radio or 802.11b Radio). The Radio Settings and Security options for the radio interface are described in the following sections.

RADIO SETTINGS

Some radio settings are available only on the 802.11a radio, as noted in the descriptions below. When you are finished configuring items on this page, click *Apply.*

- **SSID**—Enter the Service Set ID (up to 32 alphanumeric characters). Clients must set their SSIDs to match the access point. The SSID is case sensitive.
- **Closed System**— Enabling this option will not publicly broadcast the SSID.
- **Turbo Mode (802.11a only)**—Turbo Mode is an enhanced wireless LAN operating mode that can provide a higher data rate. The normal mode of the 802.11a radio provides connections up to 54 Mbps. Select *Turbo Mode Enable* to allow the radio to provide connections up to 108 Mbps.

  In normal mode the channel bandwidth is 20 MHz. In Turbo Mode the channel bandwidth is increased to 40 MHz. However, only a limited number of channels are available when Turbo Mode is enabled.

  Turbo Mode is not regulated in the IEEE 802.11a standard, and it is not allowed in some countries.
- **Radio Channel**—From the pull-down list, select the radio channel over which the access point communicates to computers in its BSS. Available channel settings are limited by local regulations that determine which channels are allowed. The client channel for wireless users is automatically set to that used by the access point to which they are linked. When multiple access points are deployed in the same area, be sure to choose channels separated by at least five channels to avoid channel interference. You can deploy up to three access points in the same area; for example, Ch1, Ch6, and Ch11.
- **Auto Channel Select (802.11g and 802.11a only)**—Select *Auto Channel Select Enable* to allow the access point to select a radio channel automatically. (Default: Enable)
- **Transmit Power (802.11g and 802.11a only)**—Set the signal strength transmitted from the access point. The longer the transmission distance, the higher the transmission power required. (Default: 100%)
- **Maximum Station Data Rate**—Select the appropriate data rate from the drop-down list for the data transfer speed running on your network. (802.11b default: 11 Mbps.) In order to reach all clients, this rate should be set lower (for example, 1 or 2 Mbps on an 802.11b radio). To isolate clients that are unable to connect at higher rates, set this value higher.
- **Beacon Interval (20-1000)**—Sets the beacon signal interval at which beacon frames are transmitted from the access point. The beacon signals allow wireless devices to maintain contact with each other. They may also carry power-management information. The Beacon Interval unit is TU, which corresponds to 1024 microseconds. (Default: 100 TU)
- **Fragment Length (256-2346) (802.11g and 802.11a only)**—The Fragment Length can be set between 256 and 2,346. If the packet size is smaller than the preset fragment size, the packet will not be segmented.

Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present, or collisions due to high network utilization, try setting the fragment size to send smaller fragments. This will speed up the retransmission of smaller frames. However, it is more efficient to set the fragment size larger if very little or no interference is present because it requires overhead to send multiple frames. (Default: 2346)

- **RTS Threshold (0-2347)**—Set the RTS (Request to Send) frame length. You may configure the access point to initiate an RTS frame sequence always, never, or only on frames longer than a specified length. If the packet size is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled.

  The access point sends RTS frames to a particular receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (Clear to Send) frame to acknowledge the right of the sending station to send data frames. The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this hidden node problem. (Default: 2346)

- **Preamble Setting (802.11g and 802.11b only)**—IEEE 802.11 frames begin with an alternating pattern of 1s and 0s called the preamble, which tells receiving stations that a frame is arriving. This provides time for the receiving station to synchronize to the incoming data stream. Enabling the Short preamble can boost your throughput; however, this can cause interoperability issues. (Default: Long)

- **Client Access Mode (802.11g only)**—802.11g radios can support both 802.11b and 802.11g clients. This option determines which mode the radio will operate in and consequently which clients will be able to connect to the radio interface. The default is to provide information for both 802.11g and 802.11b clients. Higher throughput can be achieved if the option for the 802.11g clients only is selected (since the radio is not required to transmit at the lower 802.11b rates/method).

- **Data Beacon Rate (802.11g only)**—Sets the interval at which a beacon will contain a delivery traffic indicator message (DTIM). The Access Point sends a DTIM to signal clients which are in sleep mode that a message is waiting to be delivered to them. The range for this setting is 1-255 beacons. (Default: 2)

SECURITY

The Security page allows you to set up lower-layer client authentication and data encryption parameters as described below. When you are finished configuring items on this page, click *Apply.*

CONFIGURING AUTHENTICATION

Three types of authentication can be configured:

- **Open System** (the default)—Allows access to everyone.
- **Shared Key**—If Shared Key is enabled, Encryption must also be enabled as described in "Configuring Encryption" on page 43.
- **128-Bit Dynamic Security Link**—This option can only be used with other 3Com Wireless LAN devices. The user name and password set on the access point must match those set on the clients. Each network session creates a unique, one-time encryption code.

To enable 128-bit Dynamic Security Link authentication, follow these steps:

1. Select *128-bit Dynamic Security Link.*
2. Decide whether to require Windows user authentication:

   If you check the *Require Windows user authentication* check box, clients will be required to enter a user name and password every time they associate with the network. If you leave this box unchecked, the system will authenticate clients based on the access control list and the saved passwords on the clients.
3. Create a User Access List:

   There must be at least one entry in the User Access List, which determines the users that can associate with the access point.

   Click *Edit User Access List.* In the User Access List page, user names are listed. Scroll to the bottom of the list to perform the following actions:

   To add a new user, click *Add Users.* In the next page, type the user name and password in the spaces provided and click *Apply.*

   To delete users, click *Delete Users.* In the next page, check the check boxes next to the names to be deleted and click *Apply.*

   To modify a password, click *Change Password.* In the next page, select the user name from the pull-down list. Enter the new password in the spaces provided and click *Apply.*

CONFIGURING ENCRYPTION

There are two types of data encryption available:

- WPA—Wi-Fi Protected Access.
- WEP—Wired Equivalent Privacy

The access point and the wireless devices must have the same encryption settings to communicate. You can choose to allow only clients using WPA encryption, or you can allow both WPA and WEP clients.

The following sections describe how to configure each type of encryption. When you are finished configuring the encryption, click *Apply*.

WPA Configuration

To configure WPA encryption:

1 Under WPA Configuration, click the *Required* check box if you want to limit access to clients using WPA encryption. If you also want to allow WEP clients, do not check this box.

2 Select the Cipher Mode, which determines the method by which keys are computed. WEP is the weakest Multicast Cipher Mode and is only provided for support of legacy clients which do not fully support WPA. Clients associated with WPA-TKIP will have unicast packets directed at them with corresponding encryption keys. However, with WEP selected as the Cipher Mode, ALL multicast traffic is sent out with WEP encryption. It is recommended to only select WEP as the Cipher Mode if legacy client support is critical.

AES - Advanced Encryption Standard (Highest Security)

TKIP—(Temporal Key Integrity Protocol) provides per-packet key mixing, a message integrity check and a re-keying mechanism

WEP—Provides standard WEP ciphering (Least Secure)

3 Select the type of WPA Key Management:

WPA authentication over 802.1x (More secure, but requires a RADIUS authentication server setup. **See WPA note below**)

WPA Pre-shared Key (PSK) (**see WPA note below**)

4 Select the Key Type:

Hexadecimal (0~9, A~F; for example, D7 0A 9C 7F E5)

Alphanumeric (0~9, A~F; for example 01234)

5 Enter the pre-shared key in the space provided if necessary.

WPA Note:

The WPA key management must match the settings on the Authentication Page. When using 802.1x, the access point uses session keys provided during the 802.1x EAP key exchange as the “seed key” for WPA. This is more secure than PSK, since each client starts with a unique session key for all subsequent keys generated. Otherwise, the PSK is used for the “seed key”.

The 802.1x Wireless Setup on the Authentication Page should be set as follows:

- If only one Radio is installed, and “WPA pre-shared key (PSK)” is selected on the security page, then the 802.1x Wireless Setup can be either “Disabled” or “Supported” on the Authentication Page.

-If only one Radio is installed and “WPA authentication over 802.1x” is selected on the security page, then 802.1x Wireless Setup must be either “Supported” or “Required” on the Authentication Page.

- If two Radios are installed and WPA is being used with “WPA authentication over 802.1x” selected for both radios’ WPA key management, then set the 802.1x Wireless Setup to “Required” on the Authentication Page.

-If one radio’s security is set to “WPA pre-shared key (PSK)” for WPA key management and the other is set to “WPA authentication over 802.1x”, then the 802.1x Wireless Setup must be set to “Supported” on the Authentication Page instead.

WEP Configuration

WEP encryption is based on the use of security keys and the popular RC4 encryption algorithm.

At least one transmit key must be defined in the WEP Configuration. Wireless devices without a valid WEP key will be excluded from network traffic.

The key selected as the transmit key index is used by the access point for all transmissions. Other keys defined can be used by the access point for decrypting station communications. When enabling 802.1x security with dynamic session keys, key index 4 is reserved for the 802.1x client session key. Therefore, when 802.1x clients are in the network, the access point should not be configured to use key index 4 as the transmit key index.

To configure WEP encryption:

1 Under Encryption, select *Enable.*

2 Under WEP Configuration, select the Key Size.

The access point supports shared key encryption with key lengths of 64-bits, 128-bits, or 152-bits.

3 Select the Key Type.

Hexadecimal (0~9, A~F; for example, D7 0A 9C 7F E5)

Alphanumeric (0~9, A~F; for example 01234)

3Com Passphrase(a string, described below)

4 Enter the keys in their fields.

64-bit—Each key contains 10 hexadecimal digits or 5 alphanumeric characters.

128-bit—Each key contains 26 hexadecimal digits or 13 alphanumeric characters.

152-bit—Each key contains 32 hexadecimal digits or 16 alphanumeric characters.

3Com Passphrase—This encryption string is for use only with other 3Com Wireless LAN devices. It is a case-sensitive string between 6 and 30 characters long. To enter the string, click *3Com Passphrase.* Then type any combination of letters and numbers in the Key 1 field and click *Apply.*

5 Uncheck box under WPA Configuration

6 Choose the WEP option under Multicast Cipher Mode.

HOW TO SETUP THE ACCESS POINT FOR RADIUS AUTHENTICTION

1 Using the Wireless Infrastructure Device Manger access the configuration screen for the AP8x00/AP82x0.

2 Enter your User Name and Password and click LOGIN (Default: admin with no password)

3 Select **Advanced Setup.**

4 Click on **RADIUS** from the left frame page Menu.

5 Enter all the settings of your Primary RADIUS Authentication Server (make sure the IP Address and Key match those on the RADIUS Authentication software).

6 Click on **Apply**

7 Choose **Authentication** from the left frame page Menu

8 Make sure the following settings are set on the Authentication page:

- **a** **MAC Authentication** is Disabled. (if Local or RADIUS MAC Authentication is chosen MAC address filtering or authentication, respectively, will be done before the 802.1x authentication. Therefore, these setups must be validated individually and verified functional before 802.1x can be done).
- **b** **802.1x Wireless Setup:** is set to Optional (if non-RADIUS clients need access too) or Required (if only RADIUS clients are to be allowed).
- **c** Click on Apply.

9 Click **Security** on the 802.11a/b/g radio from the left frame page Menu

10 Make sure the following settings are set from the Security page:

- **a** **Authentication** is set to Open System
- **b** **Encryption** is Enabled
- **c** **WPA Configuration** Required “Allow only WPA Clients” is left unchecked.
- **d** **Cipher Mode** is set to WEP.

e **WEP Configuration** has at least one valid WEP key.

f Click on **Apply**.

11 The Access Point is now configured for RADIUS Authentication.

How to setup the access point for WPA with 802.1x Session keys

1 Using the Wireless Infrastructure Device Manger access the configuration screen for the AP8x00/AP82x0.

2 Enter your User Name and Password and click LOGIN (Default: admin with no password)

3 Select **Advanced Setup.**

4 Click on **RADIUS** from the left frame page Menu.

5 Enter all the settings of your Primary RADIUS Authentication Server (make sure the IP Address and Key match those on the RADIUS Authentication software).

6 Click on **Apply**

7 Choose **Authentication** from the left frame page Menu

8 Make sure the following settings are set on the Authentication page:

a **MAC Authentication** is Disabled. (if Local or RADIUS MAC Authentication is chosen MAC address filtering or authentication, respectively, will be done before the 802.1x authentication. Therefore, these setups must be validated individually and verified functional before 802.1x can be done).

b **802.1x Wireless Setup:** is set to Optional (if non-RADIUS clients need access too) or Required (if only RADIUS clients are to be allowed).

c Click on Apply.

9 Click **Security** on the 802.11a/b/g radio from the left frame page Menu.

10 Make sure the following settings are set from the Security page:

a **Authentication** is set to Open System.

b **Encryption** is Enabled.

c **WPA Configuration** is Checked to “Allow only WPA Clients”.

d **Cipher Mode** is set to AES/TKIP/WEP (WEP Cipher Mode is intended ONLY for support of legacy clients. If only WPA clients are on the network, choose AES or TKIP for increased security).

e **WEP Configuration** has at least one valid WEP key.

f **WPA Key Management** set to WPA Authentication over 802.1x.

g Click on **Apply**.

11 The Access Point is now configured for WPA Authentication over 802.1x.

How to setup the access point for WPA with Pre-Shared (PSK) Key

1 Using the Wireless Infrastructure Device Manger access the configuration screen for the AP8x00/AP82x0.

2 Enter your User Name and Password and click LOGIN (Default: admin with no password)

3 Select **Advanced Setup.**

4 Choose **Authentication** from the left frame page Menu

5 Make sure the following settings are set on the Authentication page:

a **MAC Authentication** is Disabled. (if Local or RADIUS MAC Authentication is chosen MAC address filtering or authentication, respectively, will be done before the 802.1x authentication. Therefore, these setups must be validated individually and verified functional before 802.1x can be done).

b **802.1x Wireless Setup:** is set to Disabled or Optional (if RADIUS clients need access too).

c Click on **Apply**.

6 Click **Security** on the 802.11a/b/g radio from the left frame page Menu.

7 Make sure the following settings are set from the Security page:

a **Authentication** is set to Open System.

b **Encryption** is Enabled.

c **WPA Configuration** is Checked to “Allow only WPA Clients”.

d **Cipher Mode** is set to AES/TKIP/WEP (WEP Cipher Mode is intended ONLY for support of legacy clients. If only WPA clients are on the network, choose AES or TKIP for increased security).

e **WEP Configuration** has at least one valid WEP key (select the appropriate key length, key type, and key index).

f **WPA Key Management** select WPA Pre-shared Key (PSK) and Key Type.

g **Enter** the WPA PSK

h Click on **Apply**.

8 The Access Point is now configured for WPA Pre-shared Key.

WPA CONFIGURATION FOR WINDOWS XP

The following table shows how to configure the access point to support the various authentication and encryption options available for Windows XP Wireless Zero Configuration.

The following notes apply to configuring the access point for WPA under Windows XP:

- A WPA-capable wireless network interface card is required.
- The Windows XP Support Patch for Wireless Protected Access, which you can download from the Microsoft Web site, is required.
- To allow WEP clients, clear the WPA Configuration Required check box and enter an appropriate WEP key.
- For all WPA configurations, 802.1x must be enabled on the Authentication page.

Windows XP Wireless Zero Configuration		Access Points 8200/8250/8500/8700/8750		
Authentication	**Encryption**	**Authentication**	**Encryption**	**Other**
Open	Disabled	Open System	Disable	
	WEP	Open System	Enable	Enter static keys under WEP Configuration
Shared	Disabled	Not available		
	WEP	Shared Key	Enable	Enter static keys under WEP Configuration
WPA	AES	Not available on 8200		
	TKIP	Open System	Enable	WPA Configuration: Required Multicast Cipher Mode: TKIP WPA Key Management: WPA 802.1x
	WEP	Open System	Enable	WPA Configuration: Required Multicast Cipher Mode: WEP WPA Key Management: WPA 802.1x

Windows XP Wireless Zero Configuration		Access Points 8200/8250/8500/8700/8750		
Authentication	**Encryption**	**Authentication**	**Encryption**	**Other**
WPA-PSK	AES	Not available on 8200		
	TKIP	Open System	Enable	WPA Configuration: Required Multicast Cipher Mode: TKIP WPA Key Management: WPA-PSK Select Key Type and enter Pre-Shared Key
	WEP	Open System	Enable	WPA Configuration: Required Multicast Cipher Mode: WEP WPA Key Management: WPA-PSK Select Key Type and enter Pre-Shared Key

3 TROUBLESHOOTING

If you have difficulty with the 3Com Wireless LAN access point, first check the following items in the configuration:

- Radio Settings page: Ensure that the SSID is the same on clients and the access point.
- Security page: Ensure that Encryption is the same on clients and the access point.
- Authentication page: Ensure that the Local MAC Authentication System Default is set to Allow. Ensure that 802.1x Authentication Settings are correct.
- TCP/IP Settings page: If the DHCP Client is set to Disabled, then ensure that the access point IP Address is within the same subnet as the wired LAN.

If necessary, reset the access point to the factory defaults.

Try the solutions in the following table. If you need further assistance, contact 3Com Technical Support through the following Web page: http://www.3com.com/products/en_US/supportedindex.jsp

Symptom	Solutions
Access point does not power up.	Make sure the Ethernet cable is plugged into the port labeled *To Access Point* on the power brick. Check for a faulty access point power supply. Check for a failed AC power supply
Access point powers up, but has no connection to the wired network.	Make sure that the Ethernet cable is plugged into the port labeled To Hub/Switch on the power brick. Verify the network wiring and topology for proper configuration. Check that the cables used are the proper type.

Symptom	Solutions
No operation.	Verify the access point configuration. Review access point firmware revisions and update firmware if necessary. Make sure that there are no duplicate IP addresses on the network. Unplug the access point and ping the assigned address to make sure that no other device responds to that address.
Access point powers up, but does not associate with wireless clients.	Confirm that the service area on the access point matches that on the clients. Verify that the clients are operating correctly. Make sure that security settings on the access point match those on the clients. Make sure that the access point antennas are positioned properly. Check the range and move clients closer if necessary.
Mobile users do not have roaming access to the access point.	Make sure that all access points and wireless devices in the ESS in which mobile users can roam are configured to the same WEP setting, SSID, and authentication settings.
Slow or erratic performance.	Try changing the wireless channel on the access point. Check the access point antennas, connectors, and cabling for loose connections. Check the wired network topology and configuration for malfunctions.
Running on a computer connected to the wired LAN, the 3Com Device Manager cannot find an access point.	The 3Com Device Manager cannot discover devices across routers. Make sure that the computer is connected on the same segment as the access point.
After you specify an IP address for an access point, the 3Com Device Manager continues to point to the old IP address when you select the access point in the Wireless Network Tree.	In the 3Com Device Manager window click the *Refresh* button to refresh the Wireless Network Tree. Then click the access point in the Wireless Network Tree and click *Properties*. The IP address you specified is now listed. If you want to continue configuring the access point, click *Configure*.

Symptom	Solutions
While you are configuring the access point, the Configuration Management System stops responding.	To maintain wireless association, the service area and the security settings on the client and the access point must match exactly. Therefore, if you are associated with the access point that you are configuring and you change the access point service area or security, make sure to change the client service area to match. If you change the IP address and save the change, you cannot continue to configure the access point using the old IP address. Therefore, if you want to continue configuring this access point after you save this change, you must do the following: **1** Close your browser. **2** Return to the 3Com Device Manager Wireless Network Tree and click *Refresh*. **3** Select the access point and click *Configure* to start a new configuration session.
The access point cannot be configured using the Web browser.	Reset the access point (push the reset button located near the access point LEDs).

A TECHNICAL SUPPORT

OBTAINING SUPPORT FOR YOUR PRODUCT

REGISTER YOUR PRODUCT TO GAIN SERVICE BENEFITS

To take advantage of warranty and other service benefits, you must first register your product at **http://eSupport.3com.com/**. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request.

PURCHASE VALUE-ADDED SERVICES

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com Extended Warranty and Professional Services is available at **http://www.3com.com/**

WHERE TO GO FOR HELP

Contact your authorized 3Com reseller or 3Com for additional product and support information. You will find support tools posted on the 3Com web site at www.3com.com

TROUBLESHOOT ONLINE

3Com Knowledgebase helps you troubleshoot 3Com products. This query-based interactive tool is located at **http://knowledgebase.3com.com/** and contains thousands of technical solutions written by 3Com support engineers.

Connection Assistant helps you install, configure and troubleshoot 3Com desktop and server NICs, wireless cards and Bluetooth devices. This diagnostic software is located at http://www.3com.com/prodforms/software/connection_assistant/ca_thankyou.html

ACCESS SOFTWARE DOWNLOADS

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at **http://eSupport.3com.com/**.

First time users will need to apply for a user name and password. A link to softwae downloads can be found from this **http://eSupport.3com.com/** page, or located from the **www.3Com.com** home page.

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

CONTACT US

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below. You will find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

TELEPHONE TECHNICAL SUPPORT AND REPAIR

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at **http://eSupport.3com.com/**

When you contact 3Com for assistance, please have the following information ready:

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **http://eSupport.3com.com/** First time users will need to apply for a user name and password.

These numbers are correct at the time of publication. Find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim	**Telephone Technical Support and Repair**		
Australia	1 800 678 515	Philippines	1235 61 266 2602 or 1800 1 888 9469
Hong Kong	800 933 486	P.R. of China	800 810 3033
India	+61 2 9424 5179 or 000800 650 1111	Singapore	800 6161 463
Indonesia	001 803 61009	S. Korea	080 333 3308
Japan	00531 616 439 or 03 5977 7991	Taiwan	00801 611 261
Malaysia	1800 801 777	Thailand	001 800 611 2000
New Zealand	0800 446 398		
Pakistan	+61 2 9937 5083		

You can also obtain support in this region using the follwoing email,

apr_technical_support@3com.com

Or request a repair authorization number (RMA) by fax using this number: + 65 543 6348

Europe, Middle East, and Africa **Telephone Technical Support and Repair**

From anywhere in these regions, call: +44 (0)1442 435529

You can also obtain support in this region using the following URL, **http://emea.3com.com/support/email.html**

From the following countries, you may use the numbers shown:

Austria	01 7956 7124	Luxembourg	342 0808128
Belgium	70 700 770	Netherlands	0900 777 7737
Denmark	7010 7289	Norway	815 33 047
Finland	01080 2783	Poland	00800 441 1357
France	0825 809 622	Portugal	707 200 123
Germany	01805 404 747	South Africa	0800 995 014
Hungary	06800 12813	Spain	9 021 60455
Ireland	01407 3387	Sweden	07711 14453
Israel	1800 945 3794	Switzerland	08488 50112
Italy	199 161346	U.K.	0870 909 3266

Latin America: Telephone Technical Support and Repair.

You can obtain support in this region using the following URLs: Latin America.

Spanish speakers, enter the URL: **http://lat.3com.com/lat/support/form.html**

Portuguese speakers, enter the URL: **http://lat.3com.com/br/support/form.html**

English speakers in Latin America should send e-mail to: **lat_support_anc@3com.com**

Or call using the following numbers

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T+800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

North America Telephone Technical Support and Repair	1 800 876 3266

REGULATORY COMPLIANCE INFORMATION

3Com Wireless LAN Access Points 8250/8500/8750 (Models WL-450, WL462, WL-463)

FCC Radio-Frequency Exposure Notice

This device generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency radiation exposure guidelines for an uncontrolled environment, this equipment has to be installed and operated while maintaining a minimum body to antenna distance of 1 meter.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate 3Com's warranty and all applicable regulatory certifications and approvals. This product must be installed by a professional technician/installer.

FCC Part 15 Notice (Applicable to Use Within the USA)

802.11a radio only: This product is for indoor use only when using channels 36, 40, 44, or 48 (5150–5250 MHz).

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

WARNING: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

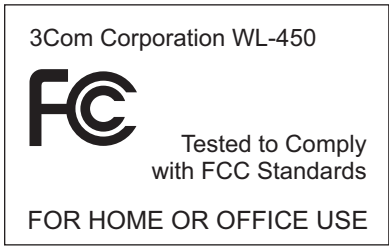
Manufacturer's Declaration of Conformity

3Com Corporation
350 Campus Drive
Marlborough, MA 01752-3064
(508) 323-5000

Declares that the product:

Date: 28 February 2003
Brand Name: 3Com Corporation
Model Number: WL-450
Equipment Type: Wireless LAN Access Point

Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Industry Canada Notice (Applicable to Use Within Canada)

This device complies with Canadian RSS-210.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's web site www.hc-sc.gc.ca/rpb.

Avis de Conformité à la Réglementation d'Industrie Canada

Pour empêcher toute interférence aux services faisant l'objet d'une licence, cet appareil doit être utilisé à l'intérieur seulement et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal.

L'installateur du présent matériel radio doit s'assurer que l'antenne est située ou pointée de manière à ce que cette dernière n'émette pas de champs radioélectriques supérieurs aux limites specifées par Santé Canada pour le grand public; consulter le Code de sécurité 6, disponible sur le site Web de Santé Canada, à l'adresse suivante: www.hc-sc.gc.ca/rpb.

Industry Canada (IC) Emissions Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conform à la norme NMB-003 du Canada.

European Community—CE Notice (WL-462, 802.11a Radio Module)

Marking by the symbol:

indicates compliance with the essential requirements of Directive 73/23/EC and the essential requirements of articles 3.1(b), 3.2 and 3.3 of Directive 1999/5/EC. Such marking is indicative that this equipment meets or exceeds the following technical standards:

- EN 301 893—Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive.
- EN 301 489-17—Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 60950—Safety of information technology equipment, including electrical business equipment.

Marking by the symbol:

indicates that usage restrictions apply.

- This product is for indoor use only when using channels 36, 40, 44, 48, 52, 56, 60, or 64 (5150–5350 MHz).
- Turbo mode is not allowed in EC countries.
- Auto Channel Select option must remain enabled to ensure product compliance with EC regulations.
- To ensure compliance with local regulations, be sure to select the country in which the access point in installed.
- This product cannot be used in Greece.
- This product can be used as shown in the table below:

Countries:	**Allowable Frequencies of Operation:**
Austria, Liechtenstein, and Switzerland.	5150–5250 MHz only (Channels 36, 40, 44, and 48).
France and Ireland.	5150–5350 MHz only (Channels 36, 40, 44, 48, 52, 56, 60, and 64).
Belgium, Denmark, Finland, Germany, Iceland, Italy, Luxembourg, The Netherlands, Norway, Portugal, Spain, Sweden, The United Kingdom.	5150–5350 MHz and 5470–5725 MHz (Channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140).

Countries:	Allowable Frequencies of Operation:
Greece.	No 5 GHz operation allowed at this time.

European Community—CE Notice (WL-463, 802.11g Radio Module)

Marking by the symbol:

CE0560 ⓘ

indicates compliance with the essential requirements of Directive 73/23/EC and the essential requirements of articles 3.1(b), 3.2 and 3.3 of Directive 1999/5/EC. Such marking is indicative that this equipment meets or exceeds the following technical standards:

- EN 300 328-2—Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques
- EN 301 489-17—Electromagnetic compatibility and Radio Spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.
- EN 60950—Safety of information technology equipment, including electrical business equipment.

Marking by the symbol:

ⓘ

indicates that usage restrictions apply.

- To ensure compliance with local regulations, be sure to select the country in which the access point in installed.
- This product can be used as shown in the table below:

Countries:	Allowed Operation:
Belgium	Indoor: Channels 1-13 Outdoor: Channel 13 only
France	Metropolitan Departments: Indoor: Channels 1-13 Outdoor: Channels 1-7 only Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte: Indoor: Channels 1-13 Outdoor: Channels 1-13 Reunion et Guane: Indoor: Channels 1-13 Outdoor: Channels 5-13 only
Italy	Indoor: Channels 1-13 Outdoor Requires license from national spectrum authority for outdoor operation.
Austria, Denmark, Finland, Germany, Greece, Iceland, Ireland, Liechtenstein, Luxembourg, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, The United Kingdom.	Indoor: Channels 1-13 Outdoor: Channels 1-13

Additional Country Restrictions (WL-463, 802.11g Radio Module)

- In Jordan, this product must be configured to operate on a legal channel. Channels 10–13 are allowed.

Consult user documentation for information on how to configure this product.

Safety Compliance Notice

This device has been tested and certified according to the following safety standards and is intended for use only in Information Technology Equipment which has been tested and certified to these or other equivalent standards:

- UL Standard 60950, 3rd Edition / CSA C22.2 No. 60950-00
- IEC 60950
- EN 60950

Published September, 2003
User Guide Version 2.3.2

INDEX

S

T

U

V

W